UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A black Samsung Galaxy Note9 smartphone, IMEI 358959099347952, in the custody and control of Homeland Security Investigations, Omaha, Nebraska.

Case No. 8:19MJ157

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of Nebraska, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1015(a) 2252A(a)(5)(B)	knowingly/makes any false statement under oath/in any matter relating to naturalization, citizenship, or registry of aliens; possession of child pornography

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DAVID K. SULLIVAN, S.A. DHS/HSI
Printed name and title

- ☐ Sworn to before me and signed in my presence.
- ☑ Sworn to before me by telephone or other reliable electronic means.

Date: 4-2-19

Judge's signature

City and state: Omaha, Nebraska

SUSAN M. BAZIS, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, David K. Sullivan, being duly sworn, hereby depose and say:

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations ("HSI"), Omaha, Nebraska, with approximately twenty-six (26) years of experience with DHS and the former Immigration and Naturalization Service, duly appointed according to law and at the time of the events herein, acting in his official capacity, and authorized to engage in or supervise the prevention, detection, investigation or prosecution of any violation of federal criminal law. I have conducted numerous child exploitation investigations and have been the affiant for numerous court-authorized arrests and search warrants. Through these investigations, my training and experience, and conversations with other agents and law enforcement personnel, I have become familiar with the methods used by individuals who produce, collect, trade, save and view child pornography.

2. I make this affidavit in support of an application for a warrant to authorize the examination of property, that is a cellular telephone, (hereinafter, **Subject Phone**) belonging to Ivan CASTILLO-Gonzalez, which is currently in law enforcement possession and that is more fully described in **Attachment A** of this affidavit, and the extraction from that property of electronically stored information by the means described in Section III of this affidavit. Based on the facts set forth in this Affidavit, I believe probable cause exists for the issuance of a warrant to search the **Subject Phone** for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely a violation of Title 18, United States Code, Sections

1015, False Statements in Connection to Naturalization, Citizenship or Alien Registry, and an attempted violation of Title 18, United States Code, Section 2252A(a)(5)(B).

3. I have not described all the facts and circumstances of which I am aware. To the extent that any information in this affidavit is not within my personal knowledge, it was made known to me through reliable law enforcement sources, and I believe it to be true. The facts contained in the ensuing paragraphs are known to me on the basis of my personal involvement in this investigation, as well as on information this Affiant obtained from other agents and officers, who are involved in this investigation, and their written reports.

I. CELLULAR PHONES AND CHILD PORNOGRAPHY

4. Through my training and experience, I have learned that cellular telephones are very often used to produce, store and transmit child pornography. A cellular telephone is a hand-held wireless device used primarily for voice communications through radio signals. These telephones send signals through networks of transmitters/receivers called "cells" enabling communication with other cellular telephones or traditional “land line” telephones. A cellular telephone usually includes a “call log” or “call history,” which records the telephone number, date and time of calls made to and from the telephone. In addition to enabling voice communications, modern cellular telephones offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic “address books”, sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; and accessing and downloading information from the Internet. The contact numbers, dates and times of contacts and text messages are often stored in the memory of these cellular telephones and can remain in storage indefinitely. Cellular telephones also may contain audio and visual

recordings, stored records of internet activity, downloaded data and e-mails. Online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. Users can set up online storage accounts from any computer or electronic device with access to the Internet. Evidence of such online storage is often found on the user's device.

5. As is the case with most digital technology, communications by way of computer or other electronic device can be saved or stored on the device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the device or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a file was previously created, stored, or shared using a device even if the original file is no longer available. Such information may be maintained indefinitely until overwritten by other data.

6. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who sexually abuse children and/or who possess, receive, distribute, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children

engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital

devices on a cyclical and repetitive basis

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. It has long been recognized by professionals dealing with persons involved with child pornography that child pornography has enduring value to those involved in the sexual exploitation of children. Such persons rarely, if ever, dispose of their sexually explicit material. Those materials are often treated as prized possessions. Individuals involved in child pornography almost always maintain their materials in a place that they consider secure

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

and where the materials are readily accessible. Most frequently, these materials are kept within the privacy and security of their own homes.

7. Your Affiant believes that given the continuing nature of this offense and the general character of such offenders as "collectors" and "hoarders", there is good reason to believe the evidence of this offense will be present on **Subject Phone.**

II. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

8. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **Subject Phone**, in whatever form they are found. One form in which the records might be found is data stored on a phone's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). Searches and seizures of evidence from computers commonly require investigators to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, computer related documentation, and peripherals) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto optical, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

III. SEARCH METHODOLOGY TO BE EMPLOYED

9. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B.**

IV. DETAILS OF THE INVESTIGATION

10. In November of 2018, DHS HSI Omaha received information from the Office of Principle Legal Advisor (OPLA) that CASTILLO had committed fraud in relation to his Form N-400, Application for Naturalization. OPLA requested investigative assistance from HSI in investigating the fraud.

11. In January of 2019, this Agent obtained and reviewed CASTILLO's alien file (A87-174-300). The alien file contained a Form N400, Application for Naturalization that had been filed by CASTILLO with United States Citizenship and Immigration Services (USCIS) on February 15, 2017. CASTILLO was interviewed by a USCIS officer, in Omaha, Nebraska under oath, regarding this Form N400 on February 26, 2018. CASTILLO confirmed that the answers he provided on the Form N400 and in his testimony were true and correct. Consequently, the USCIS officer approved the Form N400. CASTILLO was then scheduled for a Naturalization ceremony.

12. On said Form N400, Part 12, questions one through 50, ask a prospective applicant for US Citizenship several questions designed to determine the current, past and future

activities of the applicant. CASTILLO answered "No" to two specific questions, questions that were numbered 14-E and 22. These questions asked CASTILLO if he had ever been involved in "Forcing, or trying to force, someone to have any kind of sexual contact or relations" and whether he had "EVER committed, assisted in committing, or attempted to commit, a crime or offense for which [he was] NOT arrested?"

13. On April 19, 2018, CASTILLO was arrested by the Council Bluffs Police Department (CBPD) and charged with Sexual Assault in the Third Degree. On July 23, 2018, CASTILLO entered an Alford Plea to violation of the Code of Iowa, Section 709.21 Invasion of Privacy-Nudity. On August 21, 2018, CASTILLO was sentenced to two years of probation, ordered to complete sex offender treatment, required to register as a sex offender for ten years, and ordered to comply with a no contact order on behalf of the victim for a period of five years.

14. On November 23, 2018, USCIS denied CASTILLO's N400 based on a lack of "good moral character" based on his failure to disclose conduct that came to light following his arrest and conviction for crimes that occurred during the time that he was questioned about during the adjudication of the N400.

15. In January of 2019, this Agent obtained the police reports and the conviction documents for CASTILLO as a result of his arrest on April 19, 2018, where CASTILLO was arrested in Council Bluffs, Iowa and charged with Sexual Assault in the Third Degree. The victim in the investigation was CASTILLO's fifteen-year-old step daughter (YC). On April 24, 2018, YC was interviewed by Project Harmony in Omaha, Nebraska regarding the sexual assault. This Agent reviewed the Project Harmony interview. YC stated that CASTILLO had been molesting/sexually assaulting her for approximately two years, dating back to when she was in the 7th grade. YC was in 9th grade when CASTILLO was arrested in April of 2018. YC

provided the interviewer with details of what occurred during the sexual assaults, which she described as occurring frequently, under the threat of force, and as recently as April 18, 2018 (the day prior to her initial report to law enforcement).

16. Additionally, YC stated during her Project Harmony interview that CASTILLO was placing his cellular telephone in her bedroom when she was in the shower in order to video her getting dressed after she got out of the shower. YC indicated that she observed CASTILLO's cellular telephone in her room, including on her ceiling fan and in her dirty laundry bin, on multiple occasions right after she got out of the shower. YC indicated that when she observed CASTILLO's phone in her room, it was positioned in such a way that YC believed the phone was recording. YC indicated that she did not remove the cellular telephone for fear of what CASTILLO might do to her should he discover his cellular telephone was missing. YC stated that she was careful to dress under her towel when she noticed CASTILLO's cellular telephone in her room. YC indicated that after she had showered and dressed on occasions when she noticed CASTILLO's phone in her room, she would exit her room and CASTILLO would ask her to go to the basement and shut the lights off. YC indicated that when she would return to her room, CASTILLO's cellular telephone had been removed.

17. On March 18, 2019, this Affiant contacted YC and asked her what kind of cell phone CASTILLO used to hide in her bedroom. YC indicated that it was a Samsung.

18. Based on the foregoing, I believe that CASTILLO displays characteristics common to individuals who receive, distribute, and possess child pornography. For example, it is the belief of this Affiant that based on the information provided by the victim in this investigation and the investigation conducted by the Council Bluffs Police Department that

CASTILLO is attracted to minor girls approximately 14-16 years of age and that he likely still possesses images and videos of the victim on his cellular telephone.

19. On or about March 27, 2019, I learned that CASTILLO had a Samsung telephone collected as part of his property when he was detained in Saline County, Nebraska, on an arrest warrant in this matter. I seized CASTILLO's cell phone (**Subject Phone)** from property with the intention of applying for this search warrant. As such, **Subject Phone** is currently in law enforcement possession.

V. CONCLUSION

20. Based upon the above information, I believe that probable cause exists to believe there has been a violation of Title 18, United States Code, Sections 1015, False Statements in Connection to Naturalization, Citizenship or Alien Registry, and an attempted violation of Title 18, United States Code, Section 2252A(a)(5)(B), Possession of Child Pornography with Intent to View, and that evidence of those violations exist in the **Subject Phone**, which is more fully described in **Attachment A** to this affidavit.

21. In consideration of the foregoing, I respectfully request that this court issue a day time search warrant for the **Subject Phone** described in **Attachment A** authorizing the search of the aforementioned **Subject Phone** for the items described in **Attachment B** and the seizure of such items for the purpose of searching and analyzing them.

22. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will usually contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

David K. Sullivan
Special Agent
Homeland Security Investigations

Sworn to me this 2 day of April, 2019.

SUSAN M. BAZIS
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATION/DEVICE TO BE SEARCHED

A black Samsung Galaxy Note9 smartphone, IMEI 358959099347952, seized from the property of CASTILLO on March 27, 2019. The search of the device will take place in the District of Nebraska.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. All still images, videos, films, or other recordings depicting YC.

2. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including but not limited to:

> Any computer (to include cell phones and smart phones), computer system and related peripherals, including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, USB storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

3. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Any and all documents, records, text messages, emails, and internet history (in documentary or electronic form) pertaining to the sexual assault of or video voyeurism involving

YC, possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received and any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to sexually explicit conversations with a minor, or containing or pertaining to communications with minors in violation of Title 18, United States Code, Section 2422.

5. Records of or information about Internet Protocol (IP) addresses used by the computer.

6. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment.

7. Any and all evidence indicating how and when the computer(s) were accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the computer user.

8. Evidence indicating the computer user's state of mind as it relates to the crime under investigation.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A black Samsung Galaxy Note9 smartphone, IMEI 358959099347952, in the custody and control of Homeland Security Investigations, Omaha, Nebraska.

Case No. 8:19MJ157

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Nebraska
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before April 16, 2019 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to SUSAN M. BAZIS.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 4-2-19 at 2:17 p.m.

Susan M Bazis
Judge's signature

City and state: Omaha, Nebraska

SUSAN M. BAZIS, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 8:19MJ157	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION/DEVICE TO BE SEARCHED

A black Samsung Galaxy Note9 smartphone, IMEI 358959099347952, seized from the property of CASTILLO on March 27, 2019. The search of the device will take place in the District of Nebraska.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. All still images, videos, films, or other recordings depicting YC.

2. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including but not limited to:

> Any computer (to include cell phones and smart phones), computer system and related peripherals, including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, USB storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

3. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Any and all documents, records, text messages, emails, and internet history (in documentary or electronic form) pertaining to the sexual assault of or video voyeurism involving

YC, possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received and any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to sexually explicit conversations with a minor, or containing or pertaining to communications with minors in violation of Title 18, United States Code, Section 2422.

5. Records of or information about Internet Protocol (IP) addresses used by the computer.

6. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment.

7. Any and all evidence indicating how and when the computer(s) were accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the computer user.

8. Evidence indicating the computer user's state of mind as it relates to the crime under investigation.